

# EXHIBIT B

1  
2  
3  
4  
5  
6  
7  
8  
9 **UNITED STATES DISTRICT COURT**  
10 **SOUTHERN DISTRICT OF CALIFORNIA**  
11

12 HANNAH COUSIN, et al., *individually*  
13 *and on behalf of all others similarly*  
14 *situated,*

15 Plaintiffs,

16 v.

17 SHARP HEALTHCARE,

18 Defendant.  
19

Case No.: 22-cv-2040-MMA (DDL)

**ORDER GRANTING DEFENDANT’S  
MOTION TO DISMISS**

[Doc. No. 15]

20 This action consists of three consolidated cases brought by Hannah Cousin, Linda  
21 Camus, Deanna Franklin-Pittman, and Edward Barbat (“Plaintiffs”) against Defendant  
22 Sharp Healthcare (“Defendant” or “Sharp”). *See* Case Nos. 22-cv-2040-MMA (DDL),  
23 23-cv-33-MMA (DDL), 23-cv-330-MMA (DDL). On March 3, 2022, Plaintiffs filed a  
24 Consolidated Class Action Complaint alleging that Defendant intentionally disclosed its  
25 patients’ sensitive health information, without their consent, to Meta Platforms, Inc.  
26 (“Meta”) through the procurement and embedding of an internet tracking tool, Meta  
27 Pixel, on its website. Doc. No. 14 (“CAC”). On April 4, 2022, the Defendant filed a  
28 motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6). Doc. No. 15.

1 Plaintiffs filed an opposition, to which Defendant replied. *See* Doc. Nos. 17, 18. The  
2 Court found the matter suitable for determination on the papers and without oral  
3 argument pursuant to Civil Local Rule 7.1.d.1. *See* Doc. No. 19. For the reasons set  
4 forth below, the Court **GRANTS** Defendant’s motion to dismiss.

### 5 **I. BACKGROUND**<sup>1</sup>

6 Defendant is a non-profit corporation that operates multiple hospitals and medical  
7 groups, and offers a healthcare plan, throughout San Diego, California. CAC ¶ 14. One  
8 such hospital operated by Defendant is Sharp Memorial Hospital (“Sharp Memorial”).  
9 *Id.* Plaintiffs are residents of California and Sharp patients, who used Defendant’s  
10 website, www.sharp.com, to either search for health care providers, schedule medical  
11 appointments, or conduct other health care related matters. *Id.* ¶¶ 10–13, 64.

12 On June 16, 2022, “The Markup” published an article identifying Sharp Memorial  
13 as one of thirty-three hospitals across the nation that had installed and used Meta Pixel on  
14 its website. *Id.* ¶¶ 2, 32. The publication reported that Meta Pixel had collected patients’  
15 sensitive health and personal information from Defendant’s appointment scheduling page  
16 and shared it with Meta. *Id.* ¶ 3. The sensitive information included, among other things,  
17 a patient’s medical condition, prescriptions, diagnoses, and test results. *Id.* ¶ 6. “The  
18 Markup” further stated that information sent to Meta included details about patient’s  
19 medical conditions, prescriptions, doctor’s appointments, and when paired with a  
20 patient’s IP address, could be used in combination with other data to identify a specific  
21 individual or household. *Id.* ¶ 30.

22 Plaintiffs claim that Defendant failed to properly secure and safeguard their  
23 sensitive health information submitted on its website by installing and using Meta Pixel.  
24 *Id.* ¶¶ 1, 3. Plaintiffs assert that they were previously unaware of Defendant’s use of  
25

---

26  
27 <sup>1</sup> Reviewing Defendant’s motion to dismiss, the Court accepts as true all facts alleged in the  
28 Consolidated Class Action Complaint and construes them in the light most favorable to the Plaintiffs.  
*See Snyder & Assocs. Acquisitions LLC v. United States*, 859 F.3d 1152, 1157 (9th Cir. 2017).

Meta Pixel, and that their information was being shared in such a way, until after the release of this article. *Id.* ¶ 106.

Plaintiffs allege that Meta Pixel collected their sensitive information through the following process. *Id.* ¶¶ 19–29. Meta created Meta Pixel to improve their targeted advertising capability. *Id.* ¶ 19. To do this, Meta Pixel loads JavaScript code on websites and collects detailed data from interactions on the webpages. *Id.* ¶ 20. Meta Pixel tracks information from https headers and button clicks, and tracks at least seventeen standard events including payment info, registration for events, location search information, purchases, scheduling information, information that was searched for, applications, and what content users have viewed. *Id.* ¶ 24. The collected information is simultaneously delivered to Meta in “data packs” labeled with the user’s IP address. *Id.* ¶ 27. Meta then matches the information from the “data packs” with existing Facebook and Instagram profiles in a process called “advance matching.” *Id.* ¶ 28. Similarly, Meta also collects data on users without Facebook or Instagram profiles and stores it in so-called “shadow profiles.” *Id.* ¶ 29. Plaintiffs claim that, without their knowledge or consent, Defendant used Meta Pixel, as described above, to record and transmit their communications and interactions with www.sharp.com and automatically send that information to Meta. *Id.* ¶ 44.

Plaintiffs maintain that the information transmitted by Defendant to Meta included: (1) the patient’s unique and persistent Facebook ID; (2) the fact that the patient clicked on a specific medical provider’s profile page; (3) the patient’s search parameters; and (4) the patient’s location filter. *Id.* ¶ 45. As a result, Plaintiffs allege that Defendant intentionally divulged its patients’ Personally Identifiable Information (“PII”) and Protected Health Information (“PHI”) to Meta. *Id.* ¶ 51. Plaintiffs contend that Defendant divulged this sensitive patient information without obtaining their express consent and therefore violated their reasonable expectation of privacy. *Id.* ¶¶ 78, 79.

As a result, Plaintiffs bring the following five causes of action: (1) breach of fiduciary duty; (2) violation of common law invasion of privacy – intrusion upon

seclusion; (3) invasion of privacy under the California Constitution, Art. I § 1; (4) violation of the California Confidentiality of Medical Information Act, California Civil Code § 56 *et seq.*; and (5) violation of the California Invasion of Privacy Act, California Penal Code § 630 *et seq.*

## II. LEGAL STANDARD

A Rule 12(b)(6)<sup>2</sup> motion tests the legal sufficiency of the claims made in a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). A pleading must contain “a short and plain statement of the claim showing that the pleader is entitled to relief . . . .” Fed. R. Civ. P. 8(a)(2). However, plaintiffs must also plead “enough facts to state a claim to relief that is plausible on its face.” Fed. R. Civ. P. 12(b)(6); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The plausibility standard demands more than “a formulaic recitation of the elements of a cause of action,” or “naked assertions devoid of further factual enhancement.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks omitted). Instead, the complaint “must contain allegations of underlying facts sufficient to give fair notice and to enable the opposing party to defend itself effectively.” *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011).

In reviewing a motion to dismiss under Rule 12(b)(6), courts must assume the truth of all factual allegations and must construe them in the light most favorable to the nonmoving party. *See Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir. 1996). The court need not take legal conclusions as true merely because they are cast in the form of factual allegations. *See Roberts v. Corrothers*, 812 F.2d 1173, 1177 (9th Cir. 1987). Similarly, “conclusory allegations of law and unwarranted inferences are not sufficient to defeat a motion to dismiss.” *Pareto v. FDIC*, 139 F.3d 696, 699 (9th Cir. 1998). In deciding whether to dismiss the complaint for failure to state a claim, the court

---

<sup>2</sup> Unless otherwise noted, all “Rule” references are to the Federal Rules of Civil Procedure. Additionally, all citations to electronically filed documents refer to the pagination assigned by the CM/ECF system.

1 is generally bound by the facts and allegations contained within the four corners of the  
2 complaint. *Hydrick v. Hunter*, 500 F.3d 978, 985 (9th Cir. 2007).

3 Where dismissal is appropriate, a court should grant leave to amend unless the  
4 plaintiff could not possibly cure the defects in the pleading. *See Knappenberger v. City*  
5 *of Phoenix*, 566 F.3d 936, 942 (9th Cir. 2009) (quoting *Lopez v. Smith*, 203 F.3d 1122,  
6 1127 (9th Cir. 2000)).

### 7 **III. INITIAL MATTERS**

8 Plaintiffs' overarching theory of their case, underlying all claims, is that Defendant  
9 collected patients' personal and sensitive medical information on Sharp's website and  
10 that this information was then improperly shared with Meta without patients' consent.  
11 However, Plaintiffs fail to factually explain their personal participation in any of this.  
12 Plaintiffs also lump together a variety of alleged activity undertaken by Defendant, some  
13 of which is not actionable, with no meaningful factual support as to what activities each  
14 Plaintiff engaged in on Sharp's website and what information each Plaintiff provided.  
15 Therefore, the Court addresses four matters relating to the plausibility of Plaintiffs'  
16 theory of their case at the outset.

17 First, Plaintiffs allege in a conclusory manner that Defendant disclosed to Meta  
18 their personal, confidential, and sensitive medical information; communications and  
19 messages with doctors; medical test results; payment information; and, password reset  
20 information. *Id.* ¶¶ 10–13. However, these allegations are conclusory and devoid of any  
21 factual support. For example, Plaintiffs fail to factually support their contention that  
22 these activities took place. Plaintiffs also fail to allege that these activities took place on  
23 a page of Sharp's website where Meta Pixel was embedded. Further, Plaintiffs do not  
24 explain what information they provided to Defendant. Plaintiffs cannot maintain their  
25 theory of the case absent this factual support.

26 Second, Plaintiffs allege that disclosure of their browsing activity resulted in a  
27 disclosure of sensitive medical information. *Id.* However, again these allegations are  
28 unsupported factually. While Plaintiffs provide an example of a search by a hypothetical

1 patient, they fail to state what information they each provided to Defendant, via their  
2 browsing activity, that was subsequently disclosed to Meta. *Id.* ¶¶ 39–63.

3 Even assuming Plaintiffs had provided this missing information, their claims, to  
4 the extent they are based upon browsing activity, are subject to dismissal. Plaintiffs  
5 allege that they used www.sharp.com, a public website, to “research . . . doctors,” “look  
6 for providers,” and “search for medical specialists” and that through the sharing of this  
7 data, Defendant allowed Meta to collect their sensitive medical information. *Id.* ¶¶ 10–  
8 13. However, other courts have held that this type of data collection is not considered  
9 “Protected Health Information” because “nothing about [the] information relates  
10 specifically to Plaintiffs’ health” and the information is “general health information that  
11 is accessible to the public at large.” *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954–  
12 55 (N.D. Cal. 2017), *aff’d*, 745 F. App’x 8 (9th Cir. 2018). The Court therefore finds that  
13 Plaintiffs cannot maintain their claims based upon the theory that Defendant’s sharing of  
14 their browsing activity, collected on its publicly facing website, is a disclosure of their  
15 sensitive medical information.

16 Third, Plaintiffs contend that Defendant disclosed sensitive information that was  
17 collected during the appointment booking function on Sharp’s website. In support of  
18 this, Plaintiffs provide significant detail but in a hypothetical manner: Plaintiffs allege  
19 that a hypothetical patient can click on the “book appointment” button on  
20 www.sharp.com, and that Meta Pixel shared this activity with Meta, thus sharing the fact  
21 that the patient booked or attempted to book an appointment with a specific provider. *Id.*  
22 ¶¶ 51–53. Plaintiffs also allege that when a hypothetical patient clicks the direct link to  
23 call a doctor’s office, the patient’s identity and information would be shared in the same  
24 manner. *Id.* ¶¶ 54–55. Plaintiffs summarily contend that they made, booked, or  
25 scheduled appointments through Sharp’s website. *Id.* ¶¶ 10, 12, 13. But Plaintiffs do not  
26 allege that they used the “book appointment” button or used the direct link to a call a  
27 doctor’s office. *Id.* ¶¶ 10, 12, 13. Further, Plaintiffs fail to allege that these webpage  
28 interactions took them to a patient portal or otherwise plausibly conveyed their patient

status. *In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at \*26–30 (N.D. Cal. Dec. 22, 2022) (Navigating to or logging onto a healthcare provider’s patient portal differs from the general internet browsing contemplated in *Smith* because it conveys a user’s patient status which is Protected Health Information). As such, Plaintiffs fail to plausibly support their claims on this basis.

Lastly, Plaintiffs take issue with Defendant’s alleged use of Meta Pixel on Sharp’s appointment scheduling page. CAC ¶¶ 2, 3, 32. Plaintiffs claim that they used Defendant’s appointment scheduling page to “make,” “book,” or “schedule” online appointments. *Id.* ¶¶ 10, 12, 13, 64. Plaintiffs allege that Defendant required patients to “fill out medical and personal information such as the reason for the visit, name, email, phone number, address, and, as an option, [their] social security number” when creating appointments online at <https://sharp.myhealthdirect.com/bookAppointment>. *Id.* ¶ 65. Plaintiffs vaguely then conclude that they entered “sensitive personal and health information” on Defendant’s appointment scheduling page when they scheduled medical appointments online. *Id.* ¶ 66. But again, this allegation is utterly devoid of factual enhancement. Plaintiffs do not explain what personal or health information they entered on the webpage, which was then subsequently shared with Meta.

For these reasons, the Court **DISMISSES** all of Plaintiffs’ claims with leave to amend. With this in mind, the Court turns to each of Plaintiffs’ claims.

#### **IV. DISCUSSION**

##### **A. Breach of Fiduciary Duty**

Plaintiffs’ first cause of action is for breach of fiduciary duty. Plaintiffs claim that “as, a healthcare provider, Sharp has a fiduciary duty to its patients[.]” CAC ¶ 120. Plaintiffs further allege that “Sharp breached [their fiduciary] duties . . . by installing [] Meta Pixel on the appointment scheduling page and disclosing Plaintiffs’ . . . sensitive health information without their consent to Meta.” *Id.* ¶ 123. Sharp argues that Plaintiffs’ claim must be dismissed because Sharp has no fiduciary relationship with



1 Plaintiffs. Doc. No. 15 at 12–13.

2 Under California law, a breach of fiduciary duty claim requires “the existence of a  
3 fiduciary relationship, its breach, and damage proximately caused by that breach.”

4 *Pierce v. Lyman*, 3 Cal. Rptr. 2d 236, 240 (Cal. Ct. App. 1991), *superseded by statute on*  
5 *other grounds*. In order to be charged with a fiduciary obligation, a person “must either  
6 knowingly undertake to act on behalf and for the benefit of another, or enter into a  
7 relationship which imposes that undertaking as a matter of law.” *Apollo Capital Fund,*  
8 *LLC v. Roth Capital Partners, LLC*, 70 Cal. Rptr. 3d 199, 215 (Cal. Ct. App. 2007).  
9 “Whether a fiduciary duty exists is generally a question of law.” *Id.*

10 Plaintiffs allege in a conclusory manner that because Defendant is a healthcare  
11 provider a fiduciary relationship exists between Sharp and its patients. CAC ¶ 120.  
12 However, as a matter of law, there is no fiduciary relationship between Sharp and  
13 Plaintiffs. *Luiz v. Queen of Angels Hospital*, 53 Cal. App. 2d 310, 313 (Cal. Ct. App.  
14 1942) (“The relationship of hospital and patient is not per se a fiduciary or confidential  
15 one.”). The California Supreme Court has expressly held that a healthcare provider does  
16 not have a fiduciary relationship with patients and can only be held liable for a breach of  
17 fiduciary duty claim on the basis of a recognized theory of secondary liability. *Moore v.*  
18 *Regents of University of California*, 271 Cal. Rptr. 146, 153 (Cal. 1990). Accordingly,  
19 Plaintiffs fail to plausibly plead that Defendant owed them a fiduciary duty.

20 The Court is unpersuaded by Plaintiffs’ argument that the fiduciary relationship  
21 between a doctor and patient “imposes a fiduciary duty upon healthcare providers with  
22 respect to their patients as well as a duty to safeguard personal and medical information  
23 consistent with medical privacy statutes and industry standards.”<sup>3</sup> Doc. No. 17 at 4–5.

24 While Plaintiffs argue that Defendant owed its patients a duty to safeguard personal and  
25

---

26  
27 <sup>3</sup> The cases Plaintiffs cite to, *Miller v. Cal. Dep’t of Corr. & Rehab.*, No. 16-cv-02431-EMC, 2016 U.S.  
28 Dist. LEXIS 81361, at \*13 (N.D. Cal. June 22, 2016), and *Hahn v. Mirda*, 54 Cal. Rptr. 3d 527, 532  
(Cal. Ct. App. 2007), only support the proposition that as part of their fiduciary obligations, physicians  
are “prohibited from misrepresenting the nature of the patient’s medical condition.”

1 medical information, they conflate the duty of reasonable care, relevant to a claim for  
2 negligence, with the existence of a fiduciary relationship as a matter of law. *Id.* at 6–7.

3 The Court therefore **GRANTS** Sharp’s motion to dismiss Plaintiffs’ breach of  
4 fiduciary duty claim.

5 **B. Invasion of Privacy Under Common Law and the California Constitution**

6 By way of their second cause of action, Plaintiffs allege that the disclosure of their  
7 personal and sensitive health information by Sharp to Meta, via Meta Pixel, constitutes an  
8 intrusion upon seclusion. CAC ¶ 127–35. Similarly, Plaintiffs’ third cause of action is  
9 for a violation of their right to privacy pursuant to Article I, Section 1 of the California  
10 Constitution. *Id.* ¶¶ 136–44.

11 “To state a claim for intrusion upon seclusion under California common law, a  
12 plaintiff must show that: (1) a defendant ‘intentionally intrude[d] into a place,  
13 conversation, or matter as to which the plaintiff has a reasonable expectation of privacy  
14 [.]’ and (2) that the intrusion ‘occurred in a manner highly offensive to a reasonable  
15 person.’” *Davis v. Facebook Inc., (In re Facebook, Inc. Internet Tracking Litig.)* 956 F.  
16 3d 589, 601 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 97 Cal. Rptr. 3d 274,  
17 285 (Cal. 2009)). “A claim for invasion of privacy under the California Constitution  
18 involves similar elements.” *Id.* Plaintiffs must plead “that: (1) they possess a legally  
19 protected privacy interest, (2) they maintain a reasonable expectation of privacy, and  
20 (3) the intrusion [is] ‘so serious . . . as to constitute an egregious breach of the social  
21 norms’ such that the breach is ‘highly offensive.’” *Id.* (quoting *Hernandez*, 97 Cal. Rptr.  
22 3d at 285). “Because of the similarity of the tests, courts consider the claims together and  
23 ask whether: (1) there exist a reasonable expectation of privacy, and (2) the intrusion was  
24 highly offensive.” *Id.* at 601.

25 Plaintiffs contend that they had a “reasonable expectation of privacy in their  
26 sensitive health information.” CAC ¶ 130. Plaintiffs further claim that Sharp’s  
27 disclosure of their information, without their consent, “is highly objectionable to a  
28 reasonable person . . . because Plaintiffs’ sensitive health information is private and was

intended to remain private and confidential.” *Id.* ¶ 133. Defendant does not challenge Plaintiffs’ contention that they have a reasonable expectation of privacy. Instead, Defendant argues that Plaintiffs fail to sufficiently plead that the alleged invasion of privacy was “highly offensive” and that the alleged intrusion, if any, was done by a third party and not the Defendant. *See* Doc. No. 15 at 14, 19. Defendant also argues that monetary damages are not available for the alleged violation of the California Constitution. The Court addresses these arguments in turn.

*1. Highly Offensive*

In considering whether an invasion of a privacy interest is “offensive,” courts are required to consider all-inclusive “factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder’s motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive.” *Id.* at 606; *Hernandez*, 97 Cal. Rptr. at 293. The analysis of whether an invasion of privacy is “highly offensive” must also focus on the degree to which the invasion is “unacceptable as a matter of public policy.” *Id.* (citing *Hernandez*, 97 Cal. Rptr. 3d at 286) (noting that highly offensive analysis “essentially involves a ‘policy’ determination as to whether the alleged intrusion is highly offensive under the particular circumstances”).

Plaintiffs postulate that Sharp disclosed its patients’ information to Meta and that the data could be de-anonymized through the matching of Facebook IDs. But as discussed above, it is not clear that anyone has actually done so, or what information, precisely, Plaintiffs shared with Sharp that was subsequently obtained by Meta. However, it is clear that even if Plaintiffs had alleged all these facts sufficiently, disclosing a user’s browsing history does not plausibly reach the level of “highly offensive” conduct under either common law or the California Constitution. Defendant points to multiple cases holding that the collection and disclosure of a user’s browsing history and personal information on a public website is “routine commercial behavior” and not “highly offensive.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (disclosure of user’s browsing history URLs and unique ID to third party was

not highly offensive); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (disclosure of user’s personal identifying information, browsing habits, search queries, responsiveness to ads, demographic information, and declared preferences to third party was not highly offensive); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosure of unique device identifier number, personal data, and geolocation information to third party was not highly offensive). Here, while Plaintiffs generally allege that names, emails, phone numbers, addresses, social security numbers, browsing histories, and user locations were disclosed to Meta on Sharp’s public website, they do not allege they provided this information. And even reading into the Consolidated Class Action Complaint the allegations that they gave such information, none of these alleged disclosures made during routine browsing activity rise to the level of “highly offensive.”

Therefore, the Court **GRANTS** Defendant’s motion to dismiss Plaintiffs’ second and third causes of action to the extent they are based upon browsing activity.

Conversely, Plaintiffs do sufficiently plead that an alleged disclosure of sensitive health information on Sharp’s appointment scheduling page is “highly offensive.” *Katz-Lacabe v. Oracle Am., Inc.*, No. 22-cv-04792-RS, 2023 U.S. Dist. LEXIS 61306, at \*21 (N.D. Cal. Apr. 6, 2023) (holding that, in view of allegations being viewed in the light most favorable to the plaintiff, the general allegation that the defendant collected “sensitive health and personal safety information” from plaintiffs was sufficient to plead a “highly offensive” intrusion for a Rule 12(b)(6) motion).

“Courts are generally hesitant to decide claims of this nature at the pleading stage.” *In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at \*46 (N.D. Cal. Dec. 22, 2022); *See In re Facebook, Inc.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019) (“Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is.”); *In re Facebook, Inc., Internet Tracking Litig.*, 956 F. 3d at 606 (determining whether conduct was highly offensive can rarely be resolved at the pleading stage). Here,

the Court finds that Plaintiffs have alleged that disclosure of their sensitive health information on Sharp’s appointment scheduling page is “highly offensive” sufficient to withstand dismissal. CAC ¶¶ 66, 127–44. The Court therefore **DENIES** Defendant’s motion on this basis.

## 2. *Intrusion by a Third Party*

Defendant also argues that “the actual alleged intrusion upon [Plaintiffs’] seclusion, if any, [was] carried out by a third party,” which should preclude any common law intrusion upon seclusion claim against them as a matter of law. Doc. No. 15 at 15–16. However, Plaintiffs adequately and plausibly plead that Sharp intentionally intruded upon their seclusion by embedding Meta Pixel on their website and sharing their data with Meta without their knowledge or consent. CAC ¶¶ 130–33. The Court finds that Defendant’s arguments are best left for resolution at the summary judgment stage. Accordingly, the Court **DENIES** Defendant’s motion in this respect.

## 3. *Availability of Damages*

In connection with their third cause of action, Plaintiffs seek only monetary damages, not an injunction. CAC ¶ 144. Defendant contends that monetary damages are not available for an alleged violation of Article 1, Section 1 of the California Constitution. Doc. No. 15 at 19–20. Plaintiffs argue that the California Constitution “at most might not allow damages claims against governmental entities” and that “there is no such limitation for claims against private defendants.” Doc. No. 17 at 13–14.

“California’s ‘constitutional provision protecting the right of privacy . . . supports a cause of action for an injunction’ but it does not confer on a litigant a private right of action for damages.” *Moore v. Rodriguez*, No. 20-cv-01481-BAS-BGS, 2021 U.S. Dist. LEXIS 103725 at \*58–59 (S.D. Cal. June 2, 2021) (dismissing an invasion of privacy claim against private defendants under Rule 12(b)(6) because the plaintiffs only sought “damages, and not an injunction, as relief”) (citing *Clausing v. San Francisco Unified Sch. Dist.*, 271 Cal. Rptr. 72, 78, (Cal. Ct. App. 1990)). Therefore, the Court **GRANTS** Defendant’s motion to dismiss Plaintiff’s claim for monetary damages under Article 1,

Section 1 of the California Constitution.

### C. Violation of California Confidentiality of Medical Information Act

For their fourth cause of action, Plaintiffs plead that Sharp violated California’s Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq.* (“CMIA”). *Id.* ¶¶ 145–51. Specifically, Plaintiffs plead that Sharp violated section 56.10 by installing Meta Pixel on its website and disclosing patients’ medical information without their authorization. *Id.* ¶ 148. Likewise, Plaintiffs plead that Sharp violated section 56.101, by failing to preserve the confidentiality of patients’ medical information. *Id.* ¶ 149.

Defendant moves to dismiss this claim, arguing that Plaintiffs “fail[] to plead facts sufficient to show that any of their alleged medical information” was actually disclosed. Doc. No. 15 at 20–22. Additionally, Defendants contend that Plaintiffs’ claim fails because they do not allege any facts showing that anyone at Meta viewed their allegedly disclosed medical information. *Id.* at 22–23. The Court addresses both of these arguments in turn.

#### 1. Disclosure of Medical Information

CMIA prohibits the unauthorized disclosure of medical information and the negligent maintenance or preservation of medical information. Cal. Civ. Code §§ 56.10(a), 56.101(a). CMIA defines “Medical Information” as “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan . . . regarding a patient’s medical history, mental health application information, mental or physical condition, or treatment.” Cal. Civ. Code § 56.05(i). “‘Individually identifiable’ means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.” *Id.*

//



1 As discussed above, *supra* Section III, Plaintiffs have not provided sufficient facts  
2 to support the claim that their medical information was disclosed by Sharp. For this  
3 reason, the Court **GRANTS** Defendant's motion to dismiss Plaintiffs' CMIA claim.

4 2. *Viewing of Medical Information*

5 Plaintiffs must also plead that their medical information was "improperly viewed  
6 or otherwise accessed." *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 923  
7 (S.D. Cal. 2020) (citing *Regents of Univ. of Cal. v. Superior Court*, 163 Cal. Rptr. 3d 205,  
8 208 (Cal. Ct. App. 2013)). Additionally, just because medical information has been  
9 disclosed in an unauthorized manner does not mean that the information was viewed by  
10 an unauthorized person. *Id.* (citing *Sutter Health v. Superior Court*, 174 Cal. Rptr. 3d  
11 653, 661 (Cal. Ct. App. 2014)). Here, Plaintiffs only allege that data was "collected,"  
12 "stored," "sent," "delivered," "shared," or "disclosed" to Meta. CAC ¶¶ 3, 4, 27, 32, 39,  
13 90. Plaintiffs do not allege that their medical information was viewed or otherwise  
14 accessed by Meta.

15 In response, Plaintiffs argue that they only need to plead facts sufficient to infer  
16 that their medical information has been viewed by an unauthorized party. Doc. No. 17 at  
17 24. However, Plaintiffs do not provide sufficient factual allegations to make such an  
18 inference. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F.  
19 Supp. 3d 1284, 1299 (S.D. Cal. 2020) (finding that notification by the defendant of a data  
20 breach and allegations of an increase in medical related spam was enough to infer that the  
21 plaintiff's information had been viewed); *Stasi v. Inmediata Health Grp. Corp.*, 501 F.  
22 Supp. 3d at 924 (finding that the plaintiff's allegations that their information was posted  
23 on the internet was sufficient to infer the information had been viewed). Here, a single  
24 plaintiff alleges that Sharp shared her data with Meta for use in targeted advertisements.  
25 CAC ¶ 10. But this is merely a conclusion without sufficient factual support. She does  
26 not allege, for example, that she received or was subjected to an increase in any targeted  
27 advertisements. And that Meta could collect and view the information of a hypothetical  
28 patient does not support Plaintiff's claim. *Id.* ¶¶ 39–69.

Although Plaintiffs offer some additional facts in their opposition, including that Meta’s business model supports the inference that their data must have been viewed in connection with targeted marketing, Doc. No. 17 at 24–25, the Court cannot read into the Consolidated Class Action Complaint allegations that are not contained within it. *Birch v. Family First Life, LLC*, No. 22-cv-815-MMA (NLS), 2023 U.S. Dist. LEXIS 65379, at \*19 (S.D. Cal. Apr. 13, 2023); *see also Rojas v. Portfolio Recovery Assocs. LLC*, No. CV 16-9439-FMO-SSx, 2017 U.S. Dist. LEXIS 169120, at \*2 (C.D. Cal. June 7, 2017) (explaining that “an opposition is not part of a plaintiff’s pleadings”); *Barbera v. WMC Mortg. Corp.*, No C 04-3738, 2006 U.S. Dist. LEXIS 99483, at \*2 n.4 (N.D. Cal. Jan. 19, 2006) (“It is axiomatic that the complaint may not be amended by briefs in opposition to a motion to dismiss.”) (quoting *Car Carriers, Inc. v. Ford Motor Co.*, 745 F.2d 1101, 1107 (7th Cir. 1984)); *Van Buskirk v. Cable News Network, Inc.*, 284 F.3d 977, 980 (9th Cir. 2002) (“Ordinarily, a court may look only at the fact of the complaint to decide a motion to dismiss.”). Accordingly, the Court **GRANTS** Sharp’s motion to dismiss Plaintiffs’ CMIA claim for this reason as well.

#### **D. Violation of California Invasion of Privacy Act**

In their fifth cause of action, Plaintiffs allege that Sharp violated California Penal Code § 630 *et seq.*, commonly referred to as the California Invasion of Privacy Act (“CIPA”). CAC ¶¶ 152–64. In particular, Plaintiffs claim that Sharp violated section 631(a) by installing Meta Pixel on its website and scheduling page, and by facilitating Meta’s interception, recording, and storage of their information, without their consent. *Id.* ¶¶ 156–60.

Defendant moves to dismiss Plaintiffs CIPA claim on grounds that: (1) Plaintiffs fail to plausibly allege sufficient facts under California Penal Code to show Sharp “aided and abetted” Meta’s interception of any communications; (2) “Plaintiffs fail to allege facts showing ‘contents’ of communications are at issue;” and (3) any alleged interception of communications did not occur “in transit.” Doc. No. 15 at 25. The Court addresses each of these arguments in turn.



1           1.     *Sharp Aided, Agreed With, Employed, or Conspired With Meta*

2           It is clear from Plaintiffs’ pleading that they bring their CIPA claim under the  
 3 fourth clause of California Penal Code § 631(a). This subsection imposes liability on  
 4 anyone who “aids, agrees with, employs, or conspires with” someone who violates the  
 5 previous three clauses of California Penal Code § 631(a). Defendant argues that this is  
 6 “essentially the ‘aiding and abetting’ prong of the CIPA” and therefore that Plaintiffs  
 7 must sufficiently plead facts that allege Sharp “aided and abetted” under California  
 8 criminal law. Doc. No. 15 at 25–27. The Court is unpersuaded by this argument.  
 9 Defendant’s contention that “aids” means “aiding and abetting” ignores the “agrees with,  
 10 employs, or conspires with” language of the clause. Defendant provides no case law  
 11 requiring the Court to analyze “aids, agrees with, employs, or conspires with” as solely  
 12 “aiding and abetting.”

13           Plaintiffs repeatedly allege throughout their pleading that Sharp intentionally  
 14 procured Meta Pixel from Meta and installed it on their website. *See* CAC. The Court  
 15 finds that this is sufficient to plead that Sharp either aided, agreed, employed, or  
 16 conspired with Meta in the alleged interception of their information and data without  
 17 their consent. Therefore, the Court **DENIES** Defendant’s motion in this respect.

18           2.     *“Contents” of Communications*

19           “The analysis for a violation of CIPA is the same as that under the federal Wiretap  
 20 Act.” *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022)  
 21 (internal citation omitted). The Wiretap Act defines the term “contents” as “any  
 22 information concerning the substance, purport, or meaning of that communication.” 18  
 23 U.S.C. § 2510. “Contents” means “the intended message conveyed by the  
 24 communication” as opposed to “record information regarding the characteristics of the  
 25 message that is generated in the course of the communication.” *In re Zynga Privacy*  
 26 *Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014).

27           As discussed in the “Initial Matters” section above, *supra* Section III, Plaintiffs do  
 28 not provide sufficient factual support to plausibly claim their content was intercepted by

Meta as a result of installing Meta Pixel on Sharp’s webpage. Accordingly, the Court **GRANTS** Sharp’s motion to dismiss Plaintiffs’ CIPA claim on this basis.

3. *Interception “in Transit”*

CIPA § 631 applies to “communications” intercepted “in transit.” *Hammerling*, 615 F. Supp. 3d at 1092. Defendant claims that Meta Pixel creates two separate communications, one between the user’s browser and the hospital, and a second between the user’s browser and Meta. Doc. No.15 at 28. Defendant argues that since two separate communications occur, there is no interception in transit and thus Plaintiffs’ claim must fail. *Id.*

Defendant relies on *Smith*, 262 F. Supp. 3d at 951, arguing that because “the connection happens independently,” Plaintiffs have failed to sufficiently plead that communications were intercepted in transit as a matter of law. However, the *Smith* court’s analysis was limited to whether the healthcare defendants had purposefully availed themselves of conducting business in California by embedding third party code on their website. 262 F. Supp. at 951–52 (“embedding third-party code cannot confer personal jurisdiction over a website operator in the forum where the third party resides.”).

Similarly, Defendant contends that *In re Facebook Inc., Internet Tracking Litigation*, 956 F.3d at 608, should not apply here because the Northern District of California’s analysis is limited to the CIPA “party exception” rule and does not address whether other elements of CIPA were adequately pleaded. Doc. No. 15 at 29. The Court agrees that *In re Facebook Inc., Internet Tracking Litigation* is not dispositive on whether communications were intercepted in transit. 956 F.3d at 608. However, in that case the Ninth Circuit does say that “[p]ermitting an entity to engage in the unauthorized duplication and forwarding of unknowing users’ information would render permissible the most common methods of intrusion, allowing the [party] exception to swallow the rule.” *Id.*

Plaintiffs repeatedly allege that without their authorization Sharp intentionally installed Meta Pixel on its website and shared user’s information with Meta in real time.

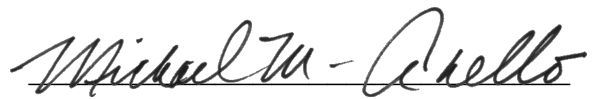
CAC ¶¶ 2–8, 19–29, 32, 152–64. Therefore, viewing the facts in the light most favorable to Plaintiffs, the Court finds that Plaintiffs plead that communications were intercepted in transit sufficient to survive dismissal under Rule 12(b)(6). Defendant’s arguments regarding what constitutes “in transit” are best left for resolution at the summary judgment stage. The Court therefore **DENIES** Defendants’ motion in this respect.

#### **V. CONCLUSION**

Based upon the foregoing, the Court **GRANTS** Sharp’s motion and **DISMISSES** Plaintiffs’ five claims with leave to amend. If Plaintiffs wish to file an amended complaint curing the deficiencies noted herein, they must do so on or before **August 2, 2023**. Any amended complaint will be the operative pleading as to Defendant, and therefore Defendant must then respond within the time prescribed by Federal Rule of Civil Procedure 15. Any claim not re-alleged in the amended complaint will be considered waived. *See* CivLR 15.1; *Hal Roach Studios, Inc. v. Richard Feiner & Co., Inc.*, 896 F.2d 1542, 1546 (9th Cir. 1989) (“[A]n amended pleading supersedes the original.”); *Lacey v. Maricopa County*, 693 F.3d 896, 928 (9th Cir. 2012) (noting that claims dismissed with leave to amend which are not re-alleged in an amended pleading may be “considered waived if not repled”).

#### **IT IS SO ORDERED.**

Dated: July 12, 2023



HON. MICHAEL M. ANELLO  
United States District Judge